

Documento de ayuda para la aplicación Segurmática Seguridad Móvil.

Índice

1. Segurmatica Seguridad Móvil	3
2. Requerimientos de instalación	3
3. Interfaz	
3.1 Pantalla Principal	3
3.2 Botón de acceso rápido	4
3.3 Análisis	5
3.4 Actualización	12
3.5 Permisos	14
3.6 Configuración	16
3.7 Soporte	21
4. Respuestas a las preguntas Frecuentes	23
5. Contactos	23

1. Segurmática Seguridad Móvil

Segurmática Seguridad Móvil es un nuevo producto orientado a la detección de aplicaciones malignas en dispositivos móviles con sistema operativo Android, entre sus principales características está el bajo consumo de recursos, que no necesita privilegios de root para ejecutarse y la posibilidad de ejecutar varios análisis simultáneamente.

2. Requerimientos de instalación

- Versiones de Android a partir de la 4.0.
- Arquitecturas ARM y x86.

3. Interfaz.

3.1 Pantalla Principal

La pantalla principal o portada de la aplicación (Figura 1.) cuenta con tres botones de acción fundamental así como un menú de navegación (Figura 2.) al que se puede acceder bien sea deslizando el dedo de izquierda a derecha o seleccionando el botón menú (Figura 3.) en la esquina superior izquierda de la pantalla. El usuario tiene la posibilidad de acceder a este menú desde cualquier pantalla de la aplicación.

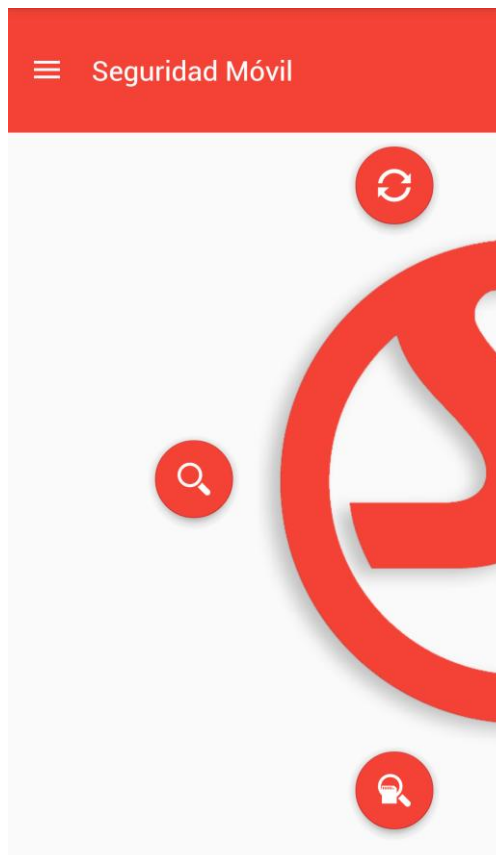


Figura 1. Pantalla Principal.

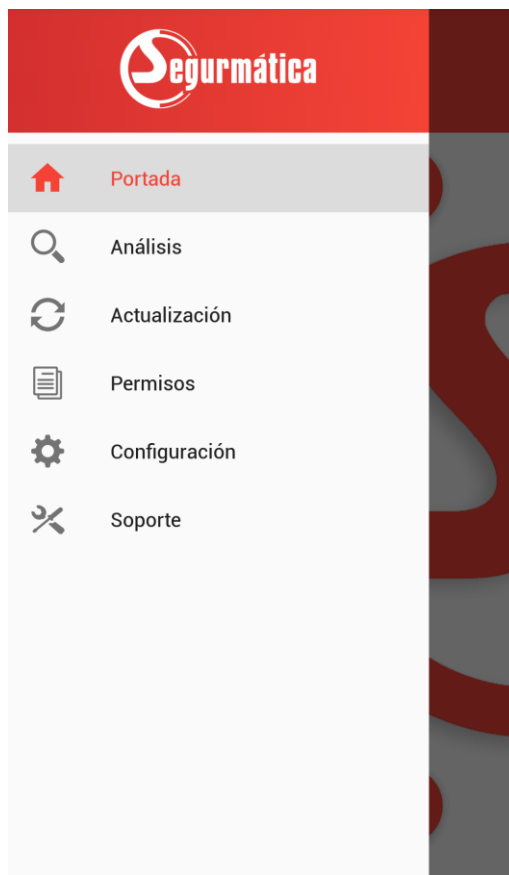


Figura 2. Menú de Navegación.



Figura 3. Botón Menú.

3.2 Botón de acceso rápido

La opción Botón acceso rápido (Figura 4.) está disponible en todas las pantallas de la aplicación excepto la pantalla principal, y tiene como objetivo que el usuario pueda acceder a las tres acciones principales de la aplicación (Analizar aplicaciones, Analizar almacenamiento y Actualizar) desde cualquier pantalla donde se encuentre.

Seleccionando este botón se muestra la pantalla de acceso rápido (Figura 5.) con las tres opciones antes mencionadas, al seleccionar una de ellas el sistema lo redirecciona automáticamente a la pantalla correspondiente al proceso iniciado ya sea un análisis o una actualización.

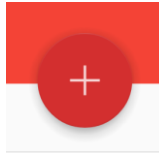


Figura 3. Botón de acceso rápido.

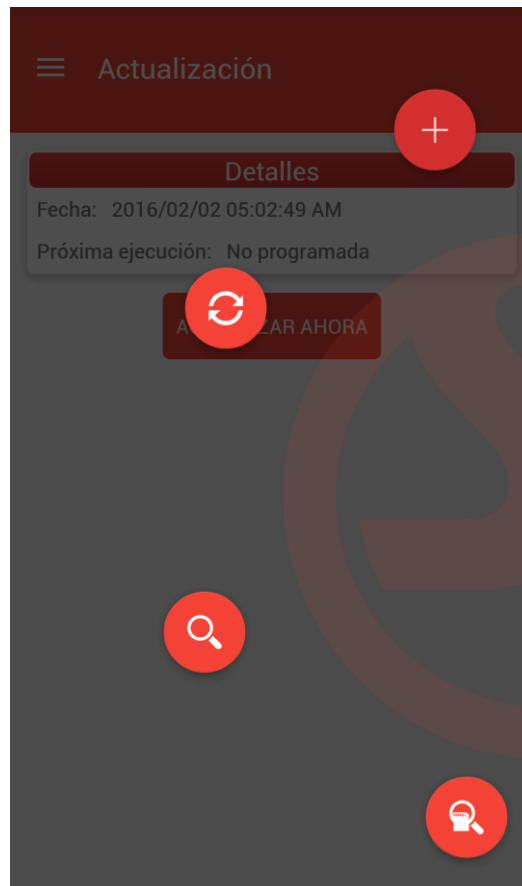


Figura 5. Pantalla de acceso rápido.

3.3 Análisis

El usuario tiene tres caminos para iniciar un análisis, estos son:

1. La pantalla de análisis (Figura 6.) a la que puede acceder desde el menú de navegación.
2. La pantalla principal que cuenta con dos botones de acceso rápido destinados a análisis.
3. La pantalla de acceso rápido que igualmente cuenta con dos botones destinados a iniciar un análisis.

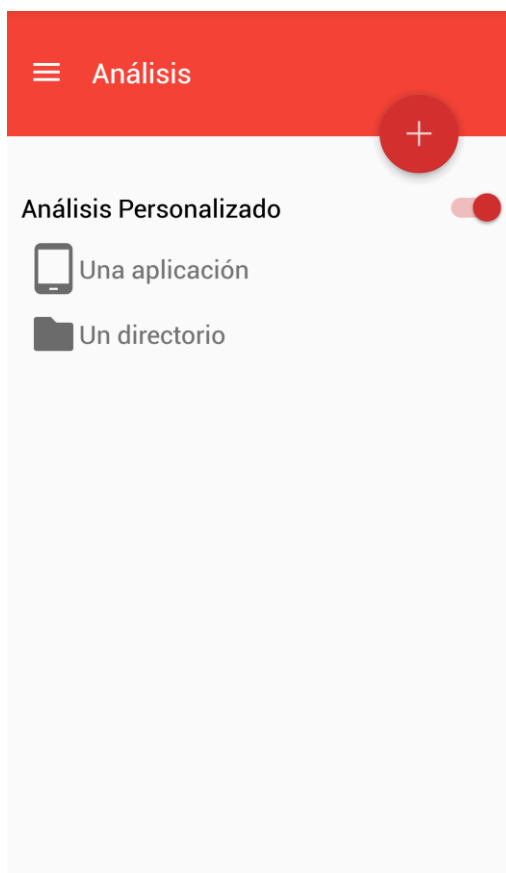


Figura 6. Pantalla de análisis.

Las opciones de análisis que abarca la aplicación son las siguientes:

- Análisis en demanda de todas las aplicaciones instaladas.
El usuario puede analizar todas las aplicaciones instaladas seleccionando el botón analizar aplicaciones (Figura 7.) que puede encontrar en la pantalla principal o en la pantalla de acceso rápido.

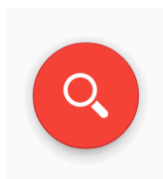


Figura 7. Botón Analizar Aplicaciones.

- Análisis automático de las nuevas aplicaciones que se instalen o se actualicen.
Habilitando en la pantalla configuración, apartado Monitor la opción “Analizar aplicaciones Instaladas”, el sistema analizará automáticamente las nuevas aplicaciones que se instalen o actualicen. En caso de que se instale o actualice una aplicación maligna el sistema de manera inmediata muestra una ventana de alerta (Figura 8.) dándole la opción al usuario de desinstalar dicha aplicación o bien ignorar y mantener la aplicación.

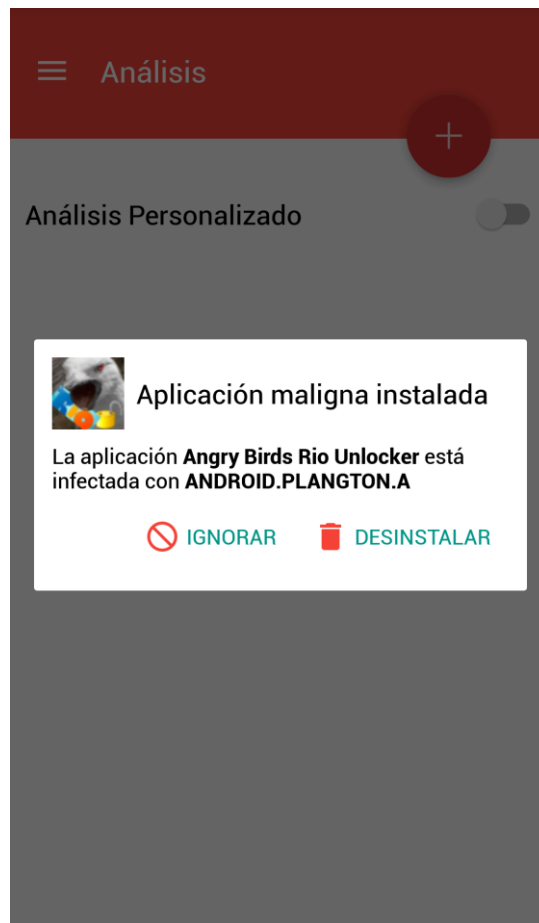


Figura 8. Ventana de Alerta. Aplicación maligna Instalada.

- Análisis de una aplicación seleccionada por el usuario de la lista de aplicaciones instaladas.

En la pantalla Análisis cuando el usuario habilita la opción Análisis Personalizado y dentro de esta selecciona el botón analizar una aplicación (Figura 9.) el sistema muestra una nueva pantalla con la lista de todas las aplicaciones instaladas en el dispositivo (Figura 10.) donde podrá seleccionar la aplicación que desee analizar.



Figura 9. Botón Analizar una Aplicación.

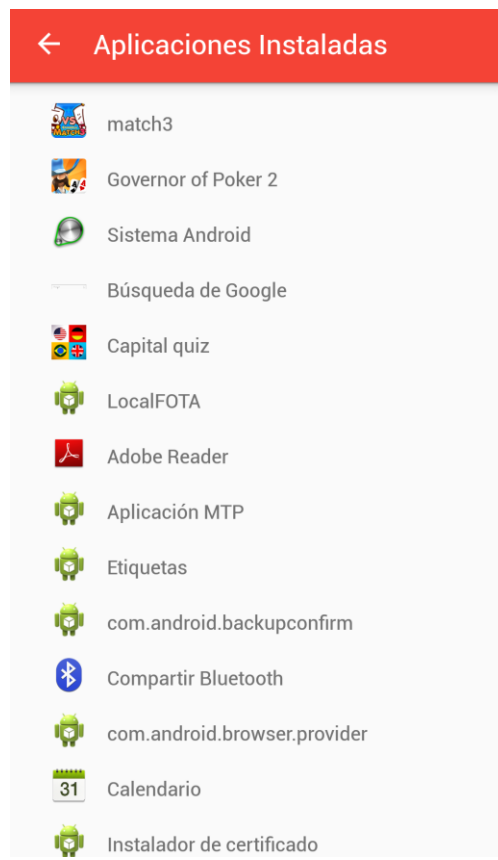


Figura 10. Lista de aplicaciones instaladas en el dispositivo.

- Análisis de un directorio seleccionado por el usuario.
En la pantalla Análisis cuando el usuario habilita la opción Análisis Personalizado y dentro de esta selecciona el botón analizar un directorio (Figura 11.) el sistema muestra un explorador de archivos (Figura 12.) que le permite navegar a través de su dispositivo y seleccionar el directorio deseado.

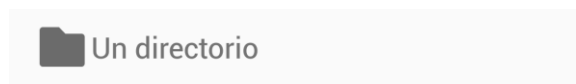


Figura 11. Botón Analizar un Directorio.

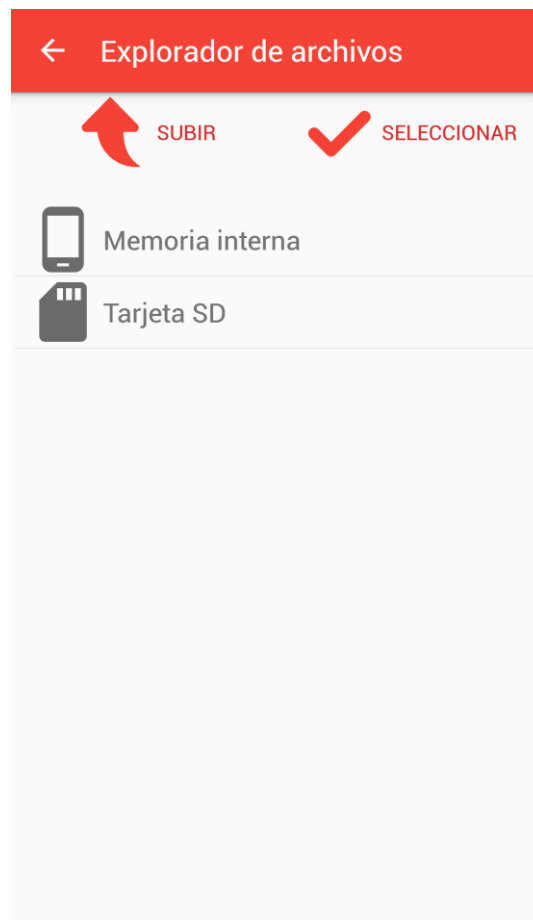


Figura 12. Explorador de Archivos.

- Análisis del almacenamiento (la memoria interna y la tarjeta micro SD).
El usuario puede analizar el almacenamiento de su dispositivo seleccionando el botón analizar almacenamiento (Figura 13.) que puede encontrar en la pantalla principal o en la pantalla de acceso rápido.



Figura 13. Botón Analizar Almacenamiento.

Una vez que el usuario inicia un análisis por cualquiera de las vías antes mencionadas el sistema lo redirecciona automáticamente a la pantalla de análisis donde podrá observar el progreso del mismo (Figura 14.), teniendo además la opción de cancelarlo si lo desea. Al terminar el análisis el sistema le muestra los resultados del mismo bien sea que no se encontraron amenazas o la cantidad de amenazas encontradas durante el análisis (Figura 15.).

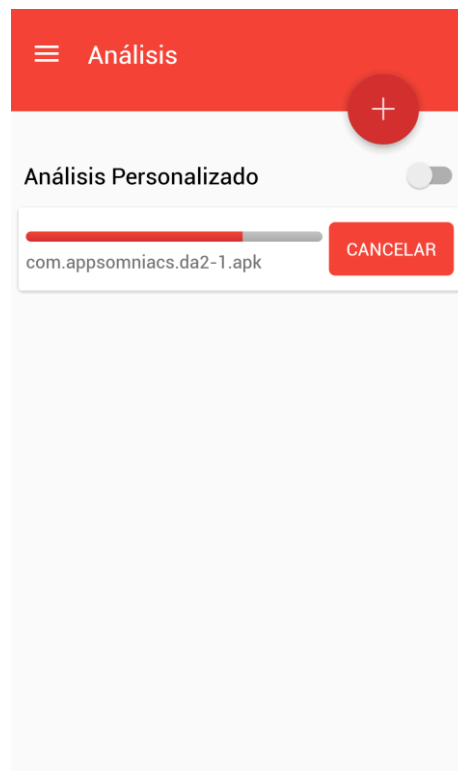


Figura 14. Progreso de un análisis iniciado por el usuario.

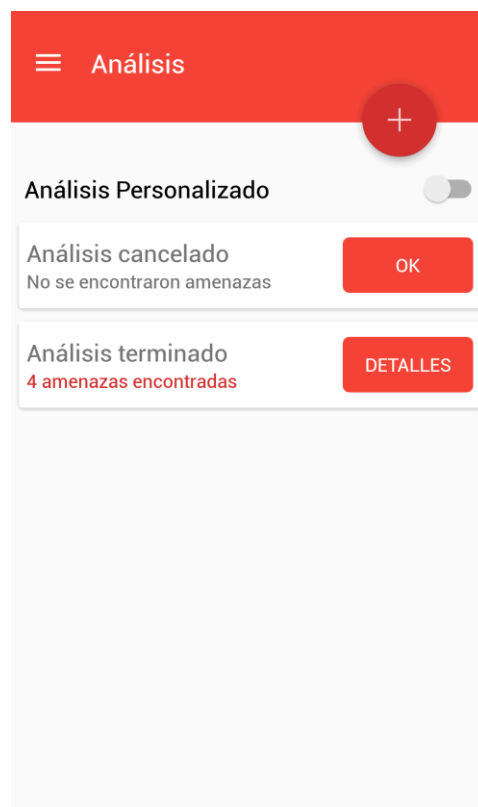


Figura 15. Resultados de análisis iniciados por el usuario.

Amenazas encontradas.

Cuando al terminar un análisis si el sistema ha detectado amenazas el usuario puede visualizar estos resultados seleccionando el botón detalles que se encuentra en cada uno de los análisis terminados con amenazas detectadas (Figura 16.) de esta forma se muestra la pantalla Resultados del análisis que varía en dependencia de la amenaza encontrada, podemos observar un listado de aplicaciones instaladas en nuestro dispositivo dándonos la posibilidad de desinstalarlas (Figura 17.) o bien un listado de ficheros malignos (.apk) dándonos la posibilidad de eliminarlos (Figura 18.). En ambos casos el usuario tendrá la opción de ignorar estos resultados.



Figura 16. Resultados de un análisis con amenazas encontradas.

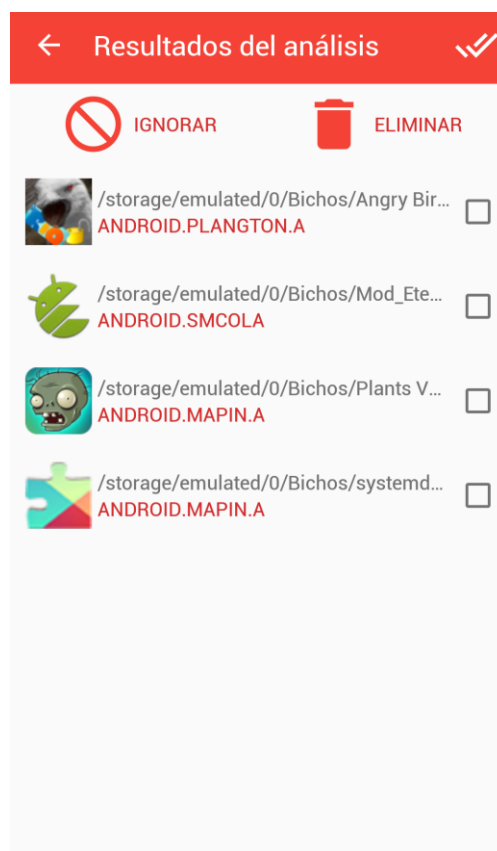


Figura 17. Pantalla Resultado de Análisis con ficheros malignos encontrados.

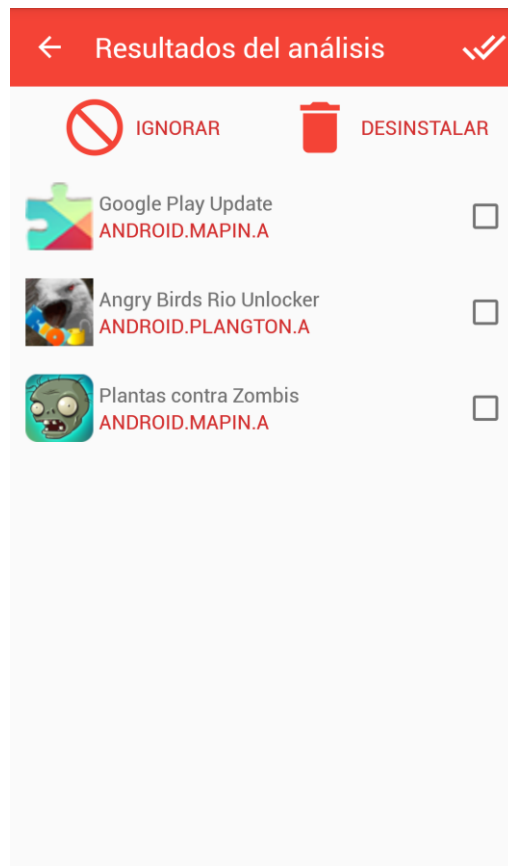


Figura 18. Pantalla Resultado de Análisis con aplicaciones malignas encontradas.

3.4 Actualización

El usuario tiene tres caminos para iniciar una actualización, estos son:

1. La pantalla de actualización (Figura 19.) a la que puede acceder desde el menú de navegación.
2. La pantalla principal que cuenta con un botón de acceso rápido destinado a la actualización (Figura 20.).
3. El menú de acceso rápido que igualmente cuenta con un botón destinado a iniciar una actualización.

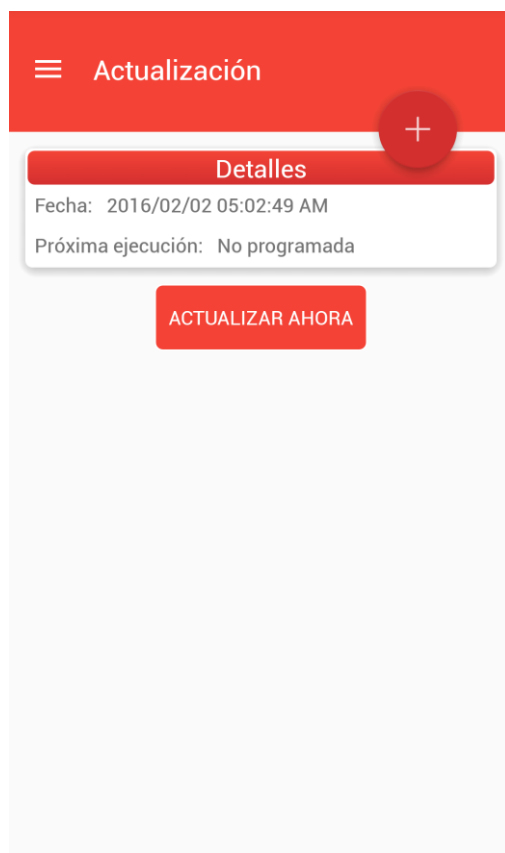


Figura 19. Pantalla de Actualización.



Figura 20. Botón Actualizar.

Para realizar una actualización desde los caminos mencionados previamente, es necesario que el usuario haya definido en la pantalla configuración, dentro del apartado Actualización los datos necesarios para el acceso al directorio de actualización y que la aplicación tenga una licencia válida.

En la pantalla Actualización el usuario puede observar los datos referentes a:

- **Fecha:** Muestra la fecha y hora de la actualización actual que tiene la aplicación.
- **Próxima ejecución:** Muestra la fecha y hora en la que está planificada la próxima ejecución del proceso actualización (Esto se define en la pantalla configuración, Apartado

Programación), en caso de no tener ninguna fecha definida el sistema muestra el cartel “No programada”.
Además cuenta con el botón Actualizar Ahora para dar inicio al proceso de actualización.

3.5 Permisos

La pantalla permisos (Figura 21.) es una pantalla meramente informativa que tiene como objetivo permitirle al usuario conocer de las aplicaciones que tiene instaladas en su dispositivo aquellas que requieren permisos que predominan en las aplicaciones malignas. En esta pantalla se muestra un listado con 10 permisos riesgosos para la seguridad de su dispositivo, seleccionando cada uno de estos se despliega un sub-listado (Figura 21.) con las aplicaciones que tienen otorgado este permiso en su dispositivo.

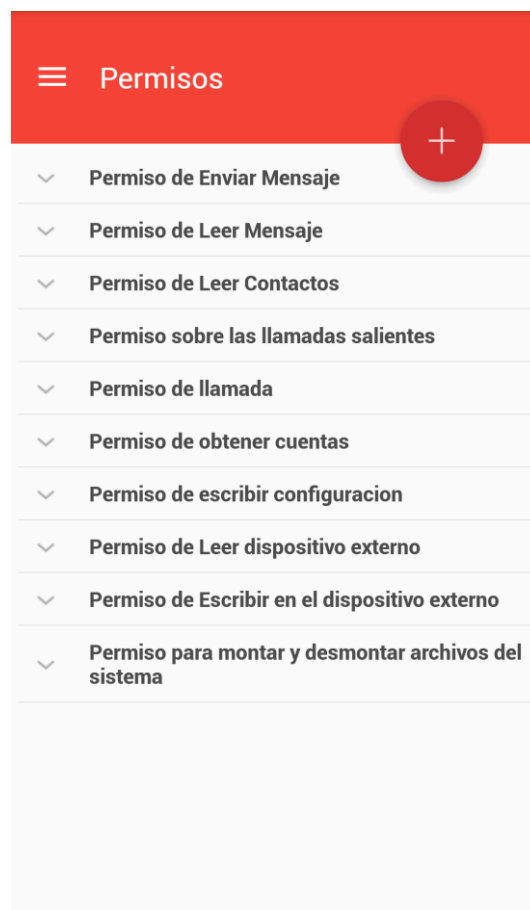


Figura 21. Pantalla Permisos.

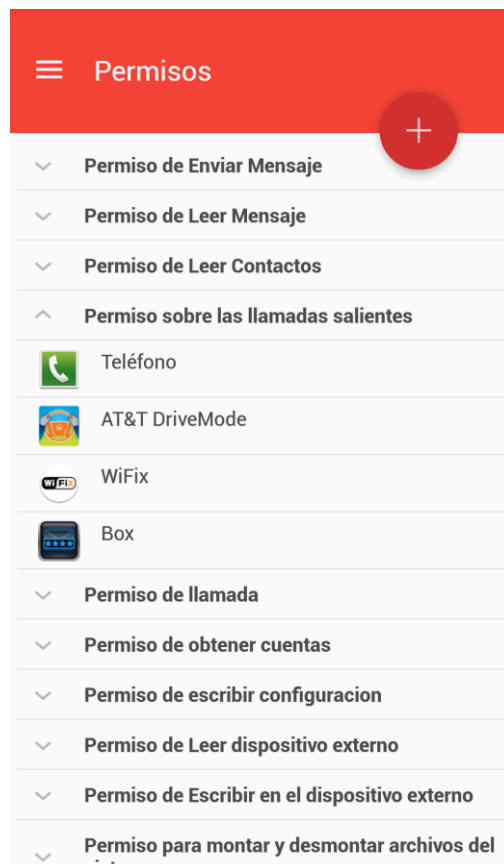


Figura 21. Pantalla Permisos. Sub-listado Permiso sobre las llamadas salientes.

3.6 Configuración

En la pantalla configuración (Figura 22.) el usuario puede encontrar los siguientes apartados:



Figura 22. Pantalla Configuración.

- **Monitor**

En este apartado el usuario tiene la opción de habilitar o no el análisis en demanda de las nuevas aplicaciones que se instalen o actualicen en el dispositivo.

Teniendo activada esta opción, cada vez que el usuario instale o actualice una aplicación el sistema analiza de manera inmediata dicha aplicación y en caso de que la misma sea riesgosa para la seguridad de su dispositivo le muestra una ventana de alerta (Figura 8), que le da la opción de desinstalar o ignorar la aplicación en cuestión.

- **Actualización**

En el apartado actualización el usuario debe definir los datos necesarios para que el sistema acceda al directorio de actualización, teniendo como opciones de origen las siguientes:

1. **Predeterminado**

Cuando se selecciona como origen la opción predeterminado el sistema se conecta automáticamente al servidor de Segurmática y muestra como opciones las pestañas “Utilizar servidor proxy” y “Actualizar solo por Wi-Fi” (Figura 23.).

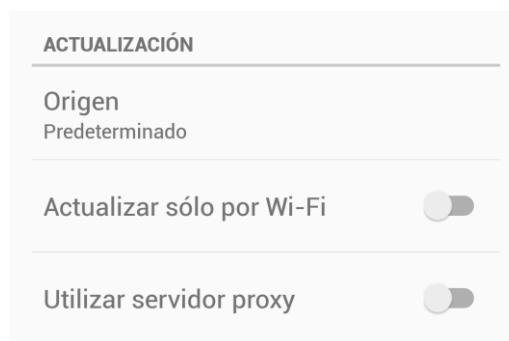


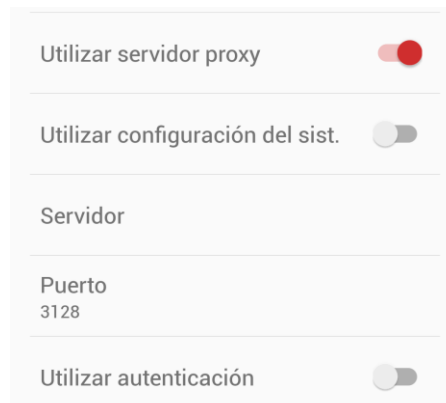
Figura 23. Pantalla Configuración. Origen Predeterminado

Habilitando “Actualizar solo por Wi-Fi” el sistema ejecutará las actualizaciones programadas siempre y cuando el dispositivo se encuentre conectado a una red Wi-Fi. En el caso de la pestaña “Utilizar servidor proxy” al habilitarla se muestra la pestaña “Utilizar configuración del sistema” (Figura 24.) que aparece por defecto habilitada de manera tal que se conecte al proxy con la configuración que ya tiene el dispositivo.



Figura 24. Pantalla Configuración. Utilizar servidor Proxy

En caso de que desee conectarse con otra configuración debe deshabilitar esta opción, con lo cual se mostrarán nuevas pestañas (Figura 25.) con datos a introducir para configurar el servidor proxy.



Utilizar servidor proxy ☒

Utilizar configuración del sist. ☐

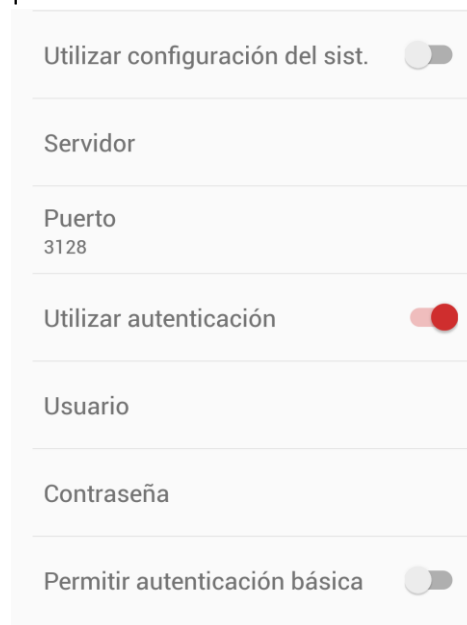
Servidor

Puerto
3128

Utilizar autenticación ☐

Figura 25. Pantalla Configuración. Utilizar configuración del sistema.

La pestaña “Utilizar autenticación” por defecto se encuentra deshabilitada, no obstante en caso de que el servidor requiera autenticación al habilitar la misma se muestran los datos necesarios a introducir (Figura 26), resaltando en este caso la pestaña “Permitir autenticación básica” que da la opción de enviar los datos en texto claro (sin cifrar) por lo que se recomienda mantenerla deshabilitada.



Utilizar configuración del sist. ☐

Servidor

Puerto
3128

Utilizar autenticación ☒

Usuario

Contraseña

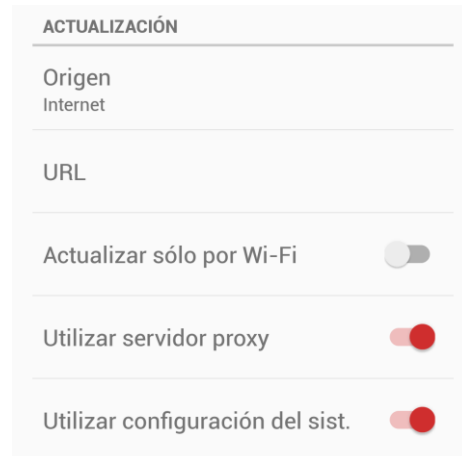
Permitir autenticación básica ☐

Figura 26. Pantalla Configuración. Utilizar autenticación.

2. Internet

Cuando se selecciona como origen la opción internet se le habilitan una serie de pestañas (Figura 27.) en el caso de la pestaña “URL” como su nombre lo indica le permite al usuario introducir la dirección url a la que desea acceder. La pestaña

“Actualizar solo por Wi-Fi”, “Utiliza servidor proxy” y “Utilizar configuración del sistema” tiene las mismas opciones y funcionamiento que se explicaron en el apartado anterior.

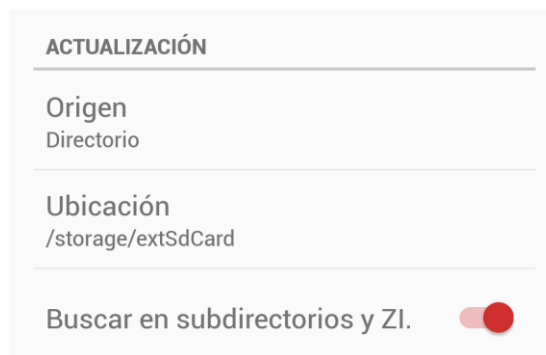


The screenshot shows the 'ACTUALIZACIÓN' settings screen. The 'Origen' (Origin) is set to 'Internet'. Below this, there is a 'URL' field. At the bottom, there are three toggle switches: 'Actualizar sólo por Wi-Fi' (disabled), 'Utilizar servidor proxy' (enabled), and 'Utilizar configuración del sist.' (enabled).

Figura 27. Pantalla Configuración. Origen Internet.

3. Directorio

Cuando se selecciona como origen la opción directorio (Figura 28.) el usuario debe seleccionar la ubicación de este directorio dentro del dispositivo, para esto cuando el usuario accede a la pestaña “Ubicación” el sistema abre el explorador de archivos a través del cual el usuario puede navegar hasta encontrar la ruta deseada y seleccionarla. También tiene la opción de habilitar o no la búsqueda en subdirectorios y ficheros zip, de manera tal que usted selecciona el directorio donde se encuentra la actualización comprimida y el sistema automáticamente detecta el fichero zip correspondiente a la actualización.

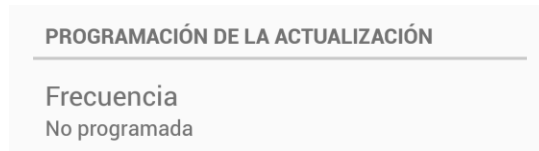


The screenshot shows the 'ACTUALIZACIÓN' settings screen. The 'Origen' (Origin) is set to 'Directorio'. Below this, there is a 'Ubicación' (Location) field showing the path '/storage/extSdCard'. At the bottom, there is a toggle switch for 'Buscar en subdirectorios y ZI.' (enabled).

Figura 28. Pantalla Configuración. Origen Directorio.

- **Programación de la Actualización**

El apartado programación de la actualización (Figura 29.) contiene las opciones destinadas a que el usuario pueda definir la frecuencia de las próximas actualizaciones. (La fecha y hora definida en este apartado se puede observar en la pantalla Análisis).



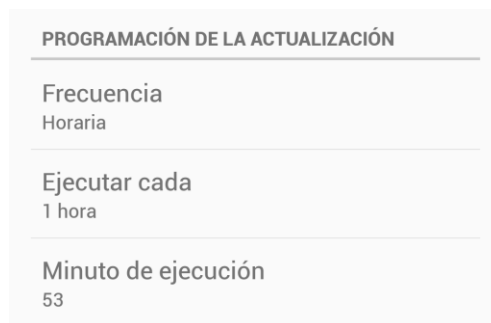
PROGRAMACIÓN DE LA ACTUALIZACIÓN

Frecuencia
No programada

Figura 29. Pantalla Configuración. Apartado Programación de la Actualización.

El sistema cuenta con 4 opciones de frecuencia:

1. No programada
Como su nombre indica, no se define una fecha de actualización automática.
2. Horaria
Cuando se selecciona esta frecuencia se muestran dos pestañas (Figura 30.) en las cuales el usuario puede definir cada cuantas horas y minutos desea se inicie el proceso de actualización de manera automática.



PROGRAMACIÓN DE LA ACTUALIZACIÓN

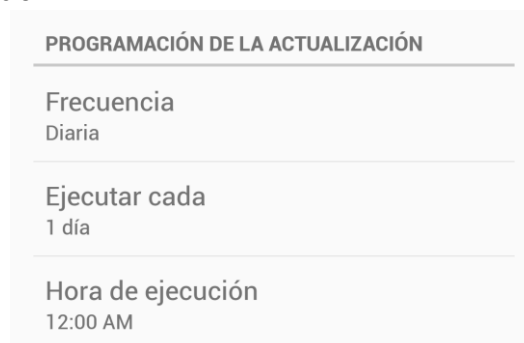
Frecuencia
Horaria

Ejecutar cada
1 hora

Minuto de ejecución
53

Figura 30. Pantalla Configuración. Frecuencia Horaria.

3. Diaria
Para el caso de la frecuencia diaria se muestran las pestañas (Figura 31.) en las cuales el usuario puede definir cada cuántos días y la hora del día en que comenzará el proceso de actualización.



PROGRAMACIÓN DE LA ACTUALIZACIÓN

Frecuencia
Diaria

Ejecutar cada
1 día

Hora de ejecución
12:00 AM

Figura 31. Pantalla Configuración. Frecuencia Diaria.

4. Semanal

La frecuencia semanal por su parte muestra las pestañas (Figura 32.) en las cuales el usuario puede definir los días de la semana así como la hora de ejecución del proceso automático de actualización.

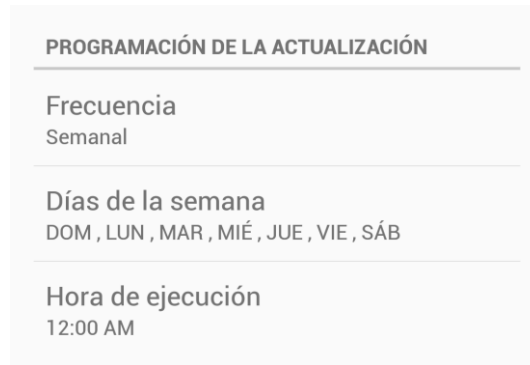


Figura 32. Pantalla Configuración. Frecuencia Semanal.

- **General**

En el apartado general (Figura 33.) el usuario tiene la posibilidad de habilitar o deshabilitar la opción “Mostrar notificación principal”.

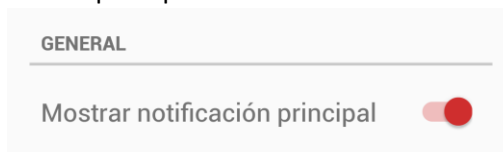


Figura 33. Pantalla Configuración. Apartado General.

Esta opción cuando está habilitada nos permite tener siempre visible el ícono de la aplicación, con la fecha de la última actualización, en la barra de notificaciones (Figura 34.).



Figura 34. Barra de notificaciones. Ícono Segurmatica Seguridad Móvil.

3.7 Soporte

La pantalla soporte (Figura 36.) contiene información sobre el producto separada en los siguientes puntos:

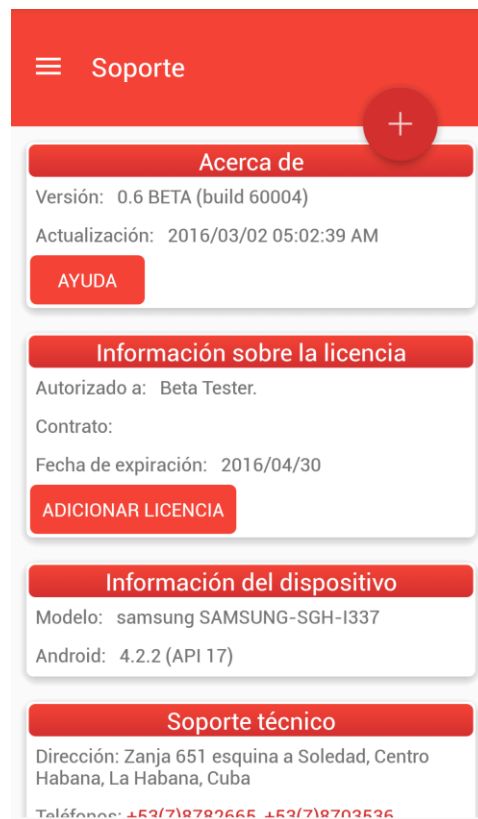


Figura 36. Pantalla Configuración. Apartado General.

- **Acerca de:** Datos de la aplicación Segurmática Seguridad Móvil como la versión de la misma, la fecha de la actualización que está utilizando así como un botón de ayuda que nos lleva a un breve recorrido por los tres botones de acción en la pantalla principal (Figura 37.).



Figura 37. Recorrido Introductorio.

- **Información sobre la Licencia:** Datos referentes a las características de la licencia que está utilizando así como un botón (Figura 38.) para seleccionar dentro del dispositivo el archivo licencia.

ADICIONAR LICENCIA

Figura 38. Pantalla Soporte. Botón Adicionar Licencia.

- **Información del dispositivo:** Muestra el modelo y versión Android del dispositivo actual.
- **Soporte técnico:** muestra los datos de contacto de nuestra entidad Segurmática (Figura 39.)



Figura 39. Pantalla Soporte. Contactos Segurmática.

4. Respuestas a las preguntas Frecuentes

5. Contactos

Empresa de Consultoría y Seguridad Informática. Segurmática

Soporte Técnico

Dirección: Zanja No. 651 esquina a Soledad, Centro Habana, Ciudad de La Habana, Cuba.

Teléfonos: +53(7) 878 2665 y 870 3536 al 38.

Telefax: +53(7) 8735965.

Email: soporte@segurmatica.cu.

Para la recepción de errores, inconformidades o sugerencias enviar correo con la plantilla de inconformidades, que puede descargar en el sitio de la entidad, y como asunto: "Aplicación Android".

Internet: <http://www.segurmatica.cu>.